

Fig. 2

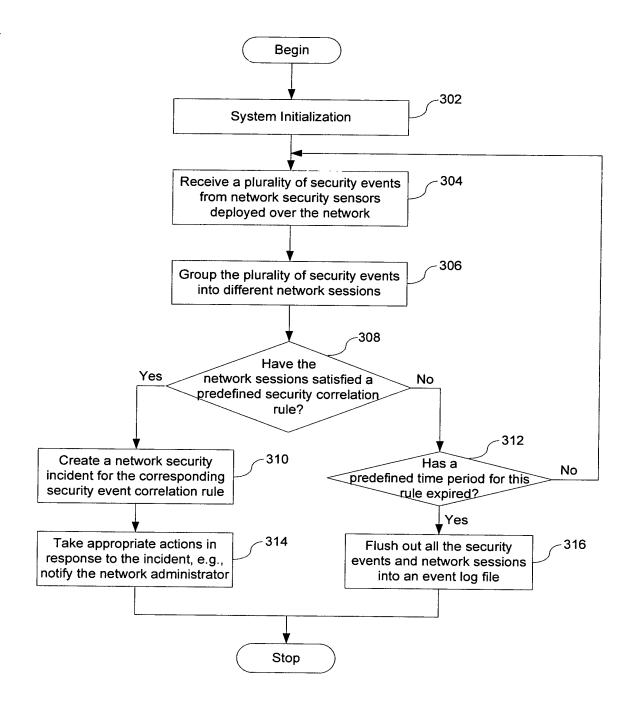
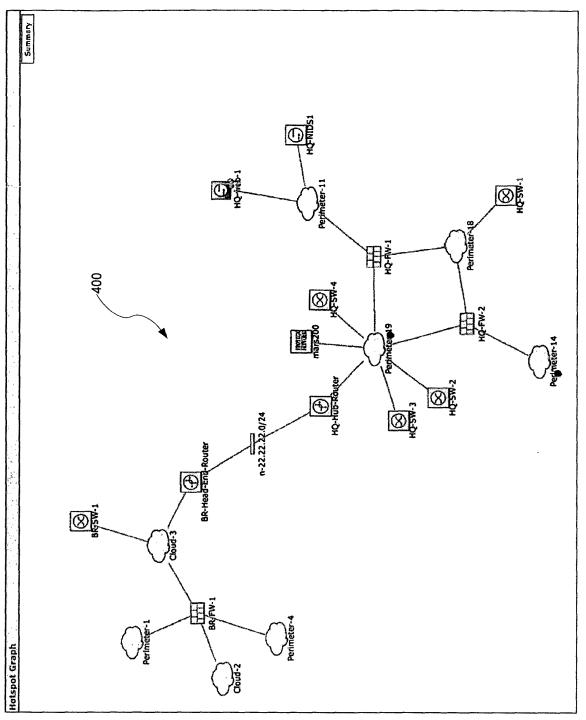
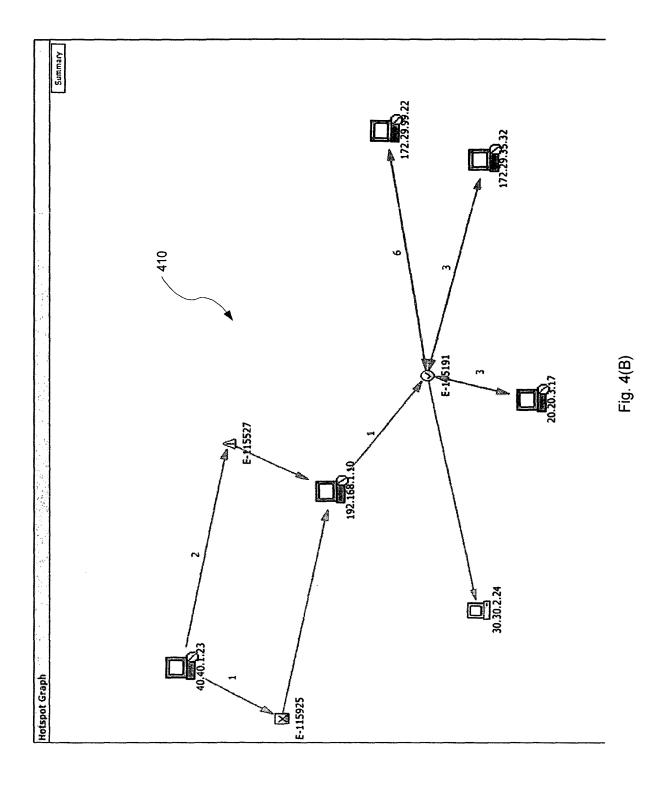
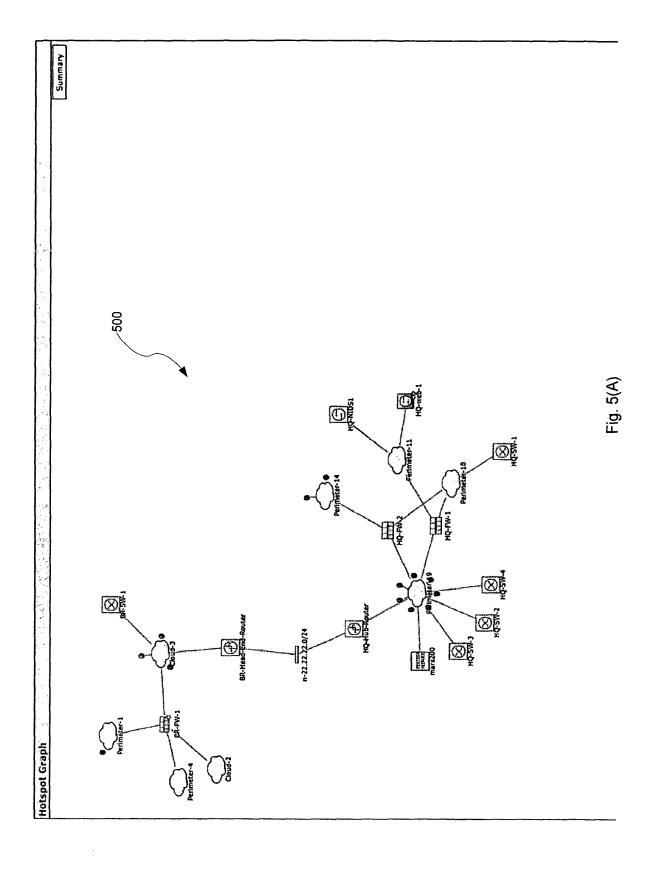


Fig. 3



rig. 4(A)





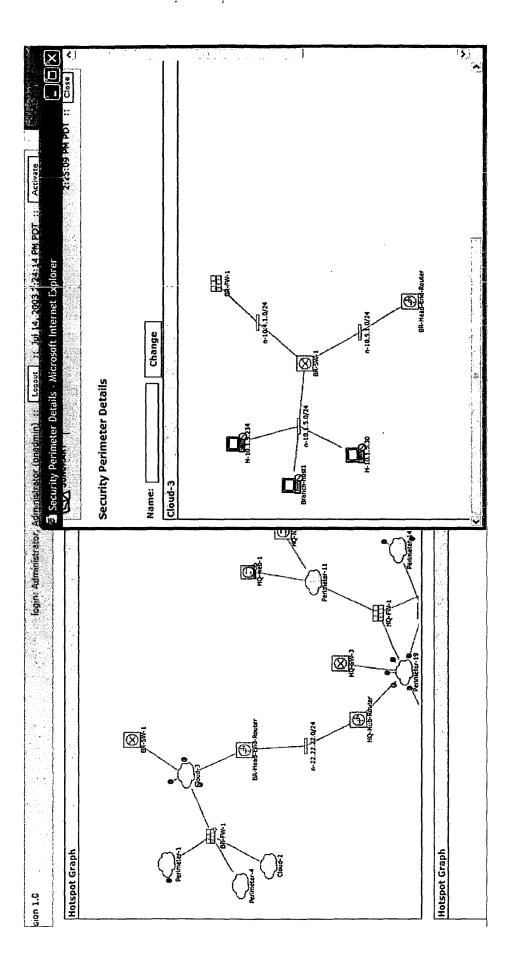


Fig. 5(B)

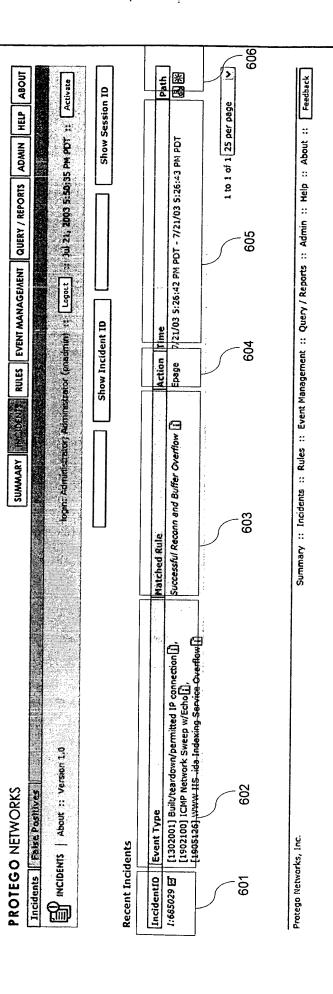


Fig. 6

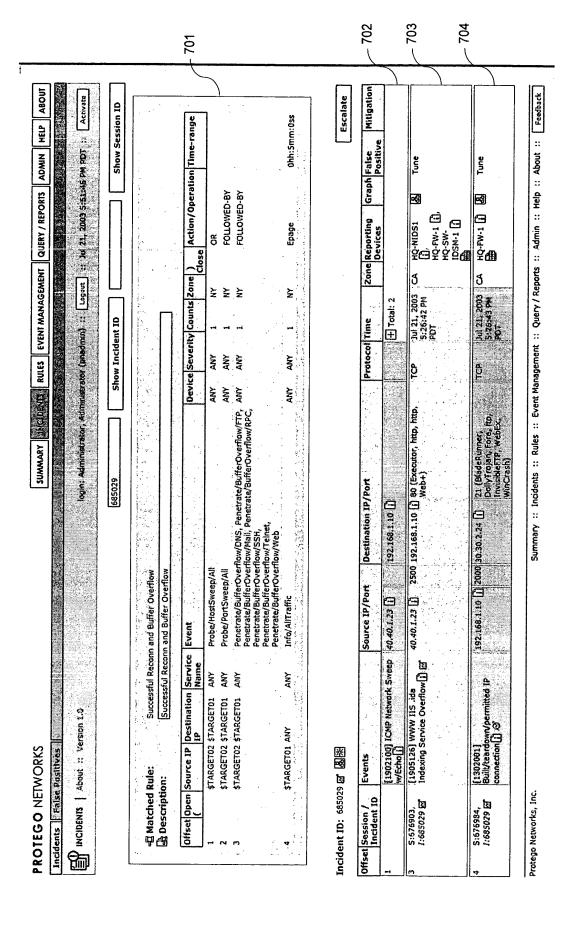


Fig. 7

Σ
ORKS
š
NETW
00
TEC
0
8

7.5

Incidents False Positives								
P INCIDENTS About :: Version 1.0	no.		logio: Administrator, Administrator (pri	Administrat	or (priadmin	A :: Ingout :: A	Logout :: 3ul 21, 2003 Si 51:45 PM PDT	f PDT ::: Acdvate
		(6)	685029	ls]	Show Incident ID	01		Show Session ID
	uccessful Re	Successful Reconn and Buffer Overflow						
B Description:	uccessful Re	Successful Reconn and Buffer Overflow		$\prod_{i=1}^{n}$				
Offset Open Source IP Destination Service Event	on Service Name	Fvent		Devic	e Severity	Device Severity Counts Zone)	Action/Operation Time-range	Time-range
1 STARGET02 STARGET01	1	Probe/HostSweep/All		AN	ANY	1 MY	ğ	
2 STARGET02 \$TARGET01	L ANY	Probe/PortSweep/All		ANY	ANY	1 187	FOLLOWED-BY	
3 \$TARGET02 \$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Penetrate/BufferOverflow/FTP, Penetrate/BufferOverflow/Naii, Penetrate/BufferOverflow/Naii, Penetrate/BufferOverflow/SSH, Penetrate/BufferOverflow/Telnet Penetrate/BufferOverflow/Neb.	inet,	ANY	ANY	I NY	FOLLOWED-8Y	
4 STARGETOI ANY	ANY	Info/AllTraffic		ANY	ANY	1 NY	Epage	Ohh:Smm:Oss

Incident ID: 685029 函 國際

Escalate

Offse	Offset Session / Events Incident ID	Events	Source IP/Port	Destination 1P/Port		rotocol Time		Zone Reporting Graph False Devices Positive	Graph Fa		Mitigation
-		(1902100) ICMP Network Sweep w/Echo[]	40.40.1.23	192.1681.10 🗍			Total: 2				
-	S:676852, I:685029 四	[1902100] ICMP Network Sweep w/Echo] 8	40.40.1.23 🗓 0	192.168.1.10 🖪 0	У	ICMP Jul 3	21, 2003 C.	10121, 2003 CA HO-SW-IDSM- B		Tune	
 4	S:676853, I:685029 🗹	[1902100] ICMP Network Sweep w/Echo[] Ø	40,40.1.23 🗓 0 192.168,1.10 🗓 0	192.168.1,10 🗓 0		OW OW	UI Z1, 2003 226:42 PM P 21	A HQ-NIDS1 []		Tune	
m	S:676903, I:665029 国	(1905126) Www IIS .ida Indexing Service Overflow[]] 画	40,40,11.23 🗍 2550	[1905126] WWW IIS ida Indexing 40.40.1.23 [] 2500 192.168.1.10 [] 80 (Executor, http://web+) Service Overflow[]] 図	Veb+) TCP	CT War and	3:26:42 PM PDT	HQ-NIDS1 [], B HQ-FW-1 [], HQ-SW-IDSM- 1 [] []	Tune	ē	
4	S:676984, J:685029 [점	[1302001] Bulltteardown/permitted IP [192.]	192,168,1,10 🗍 2000	168.1.19 [] 2000 30,30,2,24 [] 21 (BladeRunter, DollyTrojan, Fore, TCP ftp, InvisibleFTP, Webex, WinCresti)	ojan, Fore, WinCrash)		Jul 21, 2003 5:26:43 PM POT		Tune	ě	

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

PROTEGO NETWORKS		3 Security Device Information - Microsoft Internet Explorer
Incidents False Positives		PROTEGO NETWORKS
		Administrator (pnadmin) :: Jul 21, 2003 6:11:16 PM (Classification (pnadmin) :: Jul 21, 2003 6:11:16 PM (Classification Charles) (Classification C
-₫ Matched Rule: Successful Recorn a	Successful Recorn and Buffer Overflow	Security Device Information
Buccessful Reconn and Buffer Overflow	and Buffer Overflow	Name: HQ-web-1
Offset Open Source IP Destination Service Event	115	Device type: Entercept Entercept 2.5 IP Address: 192.168.1.10 None / not found.
ANY	Probe/HostSweep/All	Zone: CA Managed by: marc200[i]
ANY	Probe/PortSweep/All	
s \$TARGET02 \$TARGET01 ANY Pend Pend	Penetrate/ButterOvertlow/DNS, Pen Penetrate/BufferOverflow/Mail, Pend Penetrate/BufferOverflow/SSH, Pend	Default gateway: 0.0.0.0
ben	Penetrate/BufferOverflow/Web	Protego Networks, Inc.
STARGETO1 ANY ANY Info	nfo/AllTraffic	
Incident ID: 685029 窗 圖影		À

offs	Offset Session / Incident ID	Events	Source IP/Port Destination IP/Port		Protocol Time		Zone Reporting Graph False Devices Positive	Graph False Positive	Mitigation
]_		[1902100] ICMP Network Sweep w/Echo[i]	40.40.1.33 🕕 192.1	192.168.1.10 [])	Total: 2			
-	S:676852, 1:685029 E	[1902100] ICMP Network Sweep w/Echo[] Ø	40,40,1,23 🗓 0 192,168,1,10 🗓 0	168.1.10 🖺 0	OMP	3u 21, 2003 CA HO-SW-IDSM- B	HO-SW-IDSM-	Tune Tune	
-	S:676853, 1:685029 E	[1902100] ICMP Network Sweep w/Echo] &	40,40,1,23 D 0 192,168,1,10 D 0	68.1.10 () 0	O. O.	5:25:42 PM POT	HQ-NIDS1 []] [S]	₩ Tune	
ო	S:676903, I:685029 団	[1905126] WWW IIS .ida Indexing Service Overflow [] [3]		40.40,1.23 🗓 2500 192.168.1.10 🗓 80 (Executor, Ntp, Ntb, Web+)	ð.	ul 21, 2003 126:42 PM PDT	но-мірзі [], [§] но-ғw-1 [], но-sw-ірsм-	Tune	
4	S:676984, I:685029 🖼	[1302001] Built/teardowt/permitted I	P 192,168.1.10 [] 2000 30.30	1302g01] Built/teardown/permitted IP 192.168.1.10 [] 2000 30.30.2.24 [] [21 [BladeRunner, Doffyfrojan, Fore, TCP Jul 21, 2003 CA ponnection]] &	වු	4 21, 2063 26:43 PM PDT	. ш. — но-гw-1 🗀 🕳 🗟	Tune Tune	

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Protego Networks, Inc.

|--|

Offse	Offset Session / Incident ID	Events	Source IP/Port	Destination IP/Port	Protocol Time		Zone Reporting Graph False Devices	Graph False Positive	Mitigation
	,	[1902100] ICNP Network Sweep 40.40.1.23 w/Echo.]]	40.40.1.23	192.168.1.10 🗍		Total: 2			
	S:676852, I:685029 🖾	[1902100] ICMP Network Sweep w/Echo[] &	40.40.1.23 🖺 0	192,168,1,10 🖺 0	ICMP	33 21, 2003 5:26:42 PM PDT	Jul 21, 2003 CA HO-SW-IDSM- 图 5:26:42 PM PDT 1	Tune	
	S:676853, <i>I:685029 [</i> F]	[1902100] ICMP Network Sweep w/Echo[] &	40.40.1.23 🖺 0	0 192.168.1.10 🖺 0	ICMP	5-26-42 PM 'OT	CA HQ-NIDSI [] [8]	Tune	
m	S:676903, I:685029 편	(1995126) WWW IIS ida Indexing Service Overflow [] 图	40.40.1.23 🗓 ZSOC	(1905126) WWW IIS. idd Indexing 40,40,1.23 [] 2500 192,168,1.10 [] 80 (Executor, http, Web+) Service Overflow [] 図	a	Jul 21, 2003 5:26:42 PM PDT	A HQ-MIDSI [], [5] HQ-FW-1 [1], HO-SW-IDSM-	Tune	
4	S:676984, I:685029 図	[1302001] Built/reardown/permitted IP 192,168,11.1	192.168.1.10 []] 2000	0 30.30.2.24 [] 21 (BládeRunner, DollyTrojan, Fore- ltp, InvisibleFTP, WebEx, WinCrash)	ore. TCB	3.28:43 PM 10T	1 C B B	Tune	

正

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Protego Networks, Inc.

Offse	iffset Session / Events Incident ID	Events	Source IP/Port	IP/Port Destination IP/Port		Protocol Time Zone Reporting Graph False Mitigation	Zone Reporting	Graph F	alse M	itigation
		[1902180] ICMP Network Sweep w/Echo[]	40.40.1.23	192.168.1.10 🗍		Total: 2				
	S:676852, I:655029 🖼	[1902100] ICMP Network Sweep w/Echo [] &	40.40.1.23 🗓 0	0 192.168.1.10 🗓 0	3	ICMP Jul 21, 2003 CA HO-SW-IDSM- 配 5:26:42 PM PDT 1 引 開	CA HO-SW-IDSM-		Tune	
	S:676853, I:685029 [편	[1902100] ICMP Network Sweep w/Echo[] &	40,40,1,23 🗓 0	40.401.23 🗓 0 192.168.1.10 🗓 0		ICMP Jul 21, 2003 CA 5,26:42 PM PDT	CA HQ-NIDS1 [] [3]		Tune	
m	S:676903, I:685029 団	(1905126) www IIS ida Indexing Service Overflow]] 留	40.40.1.23 🚺 2500	[1905126] WWW IIS Jida Indexing 40.40.1.23 [] 2500 192.168.1.10 [] 80 (Executor, http, http, Web+) TCP Service Overflow[] 留	(eb+)	2P Jul 21, 2003 CA 5:25:42 PH PDT	CA HQ-NIDS1 D, B		Tune	
А	S:676984, I:685029 II	[1302001] Bull/Leardown/permitted IP '192.168. connection[] @	192,168-1,10 [] 2000	8.1,10 [] 2000 30.30,2,24 [] 21 (BedeRunner, CollyTrojan, Fore, RCP ftp, InvisibleTTP, Webex, WinCrash)	yan, Fore, VinCrash)	5P M. 23, 2003 CA 5:25,43 PM PDT	CA HQ-FW-1 [] [] [] []		Tune	

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Fig. 11(A)

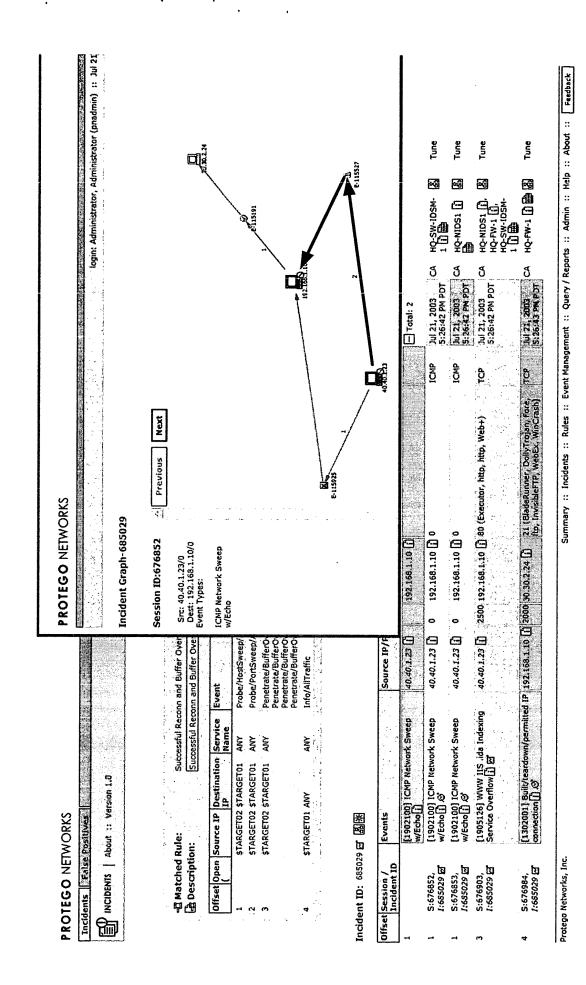


Fig. 11(C)

False Mitigation	**************************************	Tune	Tune	Tune	Tune
Graph					
Zone Reporting Graph False Devices Positive		3.26:42 PM FDT CA HO-SW-IDSM- B	HQ-NIDS1	HQ-NIDS1 [], [S] HQ-FW-1 [], HQ-SW-IDSM- 1 [] [но-гм-1 🗋 🖨 🖾
Zone		2	ర	<u>გ</u>	್ರ ∴೯!
	Total: 2	Jul 21, 2003 5:26:42 PM PD	3.4 21, 2003 5.26:42 PM 10	TCP 30/21, 2003 5:26:42 PM FDT	14 21, 2003 CA 5.26:43 PM FDT
Protocal Time		ICMP	ICMP	ð	
Source IP/Port Destination IP/Port	40.40.1.23 [] 192.168.1.10 [] -		40.40.1.23 [] 0 192.168.1.10 [] 0	1905126) WWW IIS .ida Indexing	d IP 192.188.1.10 []] 2000 30.30.2.24 [] 21 (BladeRunner, Dollyrojan, Fore, ITCP (to, InvisibleTP, WebEx, WinCrash)
Events	[1902100] ICMP Network Sweep w/Echo	[1902100] ICMP Network Sweep w/Echo[] &	(1902100) ICMP Network Sweep w/Echo[] &	[1905126] WWW IIS .ida Indexing Service Overflow[]] Ef	(1302001) Built/heardown/permitted IP 192,168.
Offset Session / Incident ID		S:676852, I:685029 🖼	S:676853, I:685029 🗹	S:676903, I:685029 편	S:676984, I:685029 ⊞
offs			 '	m	4

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Fig. 12(B)

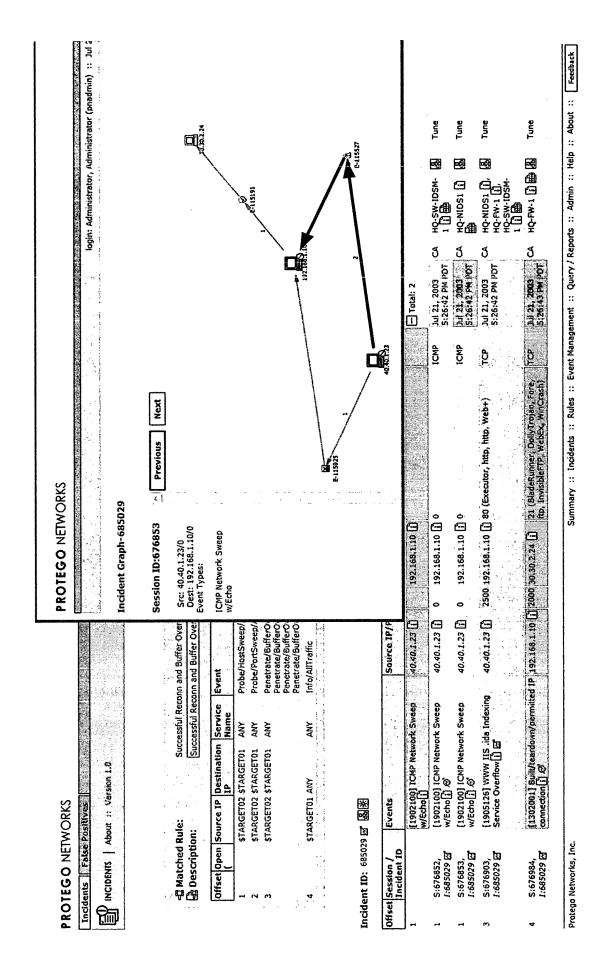


Fig. 12(C)

PRO	PROTEGO NETWORKS		🗿 Raw Events - Mi	w Events - Microsoft Internet Explorer	Explorer	de de l'automotion (All A. Carlo de décados de la compre devolution de descent	And the same of th		X ADMIN	N HELP ABOUT	巨
	ents Fals	Incidents FelisePositives	Raw Events	ارسید مسیدن در درساز بازی درساز درس	رغادارتار دوست والأسود فادار ساهت سيطالك		reached appropriate of the company o		TOW NO ST	DT :: Activate	
			Event / Session / Incident 10	Reporting Device	Time	Raw Message		-	She	Show Session ID	
	न्द्र Matched Rule: क्रि Description:	Rule: Successful Reconn and B Successful Reconn and B	E:676903, S:676903, I:685029 図	HQ-FW-1	Jul 21, 2003 5:26:42 PM POT	10.33.10.2 <142>%PIX-6-302013: Bult inbound TCP connection 2055 for outside:40.40.1.23/2500 (40.40.1.23/2500) to dmz:192.168.1.10/80 (100.1.4.10/80)	(40.40.1.23/2500) to dmz	connection 2055 ::192.168.1.10/80	· · · • ·		
	Offset Open	Offset Open Source IP Destination Service Event	E:676905, S:676903, <i>I:685029</i> 🖼	HQ-FW-1	Jul 21, 2003 5:26:42 PM PDT	10.33.10.2 <142>%p1X-6-302014: Teardown TCP connection 2055 for outside:40.40.1.23/2500 to dmz:192.168.1.10/30 duration 0:00:22 bytes 752 TCP Reset-O	32014: Teardown TCP con Imz:192.168.1.10/30 dura	inection 2055 for stion 0:00:22	tion T	tion Time-range	
•	- 12	ANY	E:676901, S:676903, I:685029 國	HQ-FW-1	Jul 21, 2003 5:26:42 PM PDT	10.33.10.2 <141>%PIX-5-304001: 40.40.1.23 Accessed URL 100.1.4.10: ida?<200+ chars>	14001: 40.40.1.23 Access	ed URL			
	m	\$1ARGE102.\$TARGET01 ANY Penetral Penetral Penetral Penetral Penetral	E:676904, S:676903, 1:685029 国	HQ-NIDS1	Jul 21, 2003 5:26:42 PM PDT	40.40.1.23/2500> 192.168.1.10/80 TCP WWW IIS .ida Indexing Service Overflow	3.1.10/80 TCP WWN 11S .	ida Indexing		· · · ·	
- I	1 2 3 3 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	STARGETOL ANY ANY Info/all	E:676900, S:676903, I:685029 国	HQ-SW- IDSM-1	Jul 21, 2003 S:26:42 PM PDT	40.40.1.23/2500> 100.1.4.10/80 TCP WWW IIS ida Indexing Service Overflow	.10/80 TCP WWW IIS .ida	Indexing Service	5	0hh:Smm:0ss	
Incide	Incident ID: 685029 召 B账	29 窗 屬腦	Protego Networks, Inc.	inc.				Feedback	?	Escalate	
Offset	Offset Session / Incident ID	Events	Source IP/Port 0	Destination IP/Port	1400	toud.	Protocol Time Zor	Zone Reporting Devices	Graph False Positi	False Mitigation Positive	E
		(1902100) ICMP Network Sweep 40-40 w/Echo]]	1 0 62.1.00.00	192,168,1,10			☐ Total: 2				7
	S:676852, 1:685029 🖼	[1902100] ICMP Network Sweep 40.40 w/Echo[]] Ø	40.40.1.23 🗓 0 19	192.168.1.10 🖺 0		ICMP	Jul 21, 2003 CA 5:26:42 PM PEFT	HO-SW-IDSM-	Mar Tune		
-	S:676853, 1:685029 🖼	[1902100] ICMP Network Sweep 40.46 w/Echo[]] Ø	40.40.1.23 🗓 0 19	192.168.1.10 🗓 0		A STATE OF THE STA	S126:42 PM PUT	HQ-NIDS1	Tune		
m	S:676903, 1:685029 🖼	[1905126] WWW IIS .ida Indexing 40.40 Service Overflow[] 🖼	40.40.1.23 🗓 2500.192.168.1.10 🗍 80 (Executor, http, http, Web+)	2.168.1.10 🖺 BI	0 (Executor, http	, http://web+)	Jul 21, 2003 CA 5:26:42 PM PET	HQ-NIDS1 [],	Tune		
4	S:676984, I:685029 🖼	[1302001] Bultreardown/permitted IP 192, 1667.	68.1.10 🗓 2000 3	30.2.24 [] [2]	I (BladeRunner, p, InvisibleFTP,	10 [] 2000 30,30,2.24 [] [21 (BladeRunner, CollyTrojan, Fore, TCP	IN 21, 2003 CA	HQ-SW-1DSM- 1 DBB HQ-FW-1 DBB	Tune		

Fig. 13(A)

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Fig. 13(B)

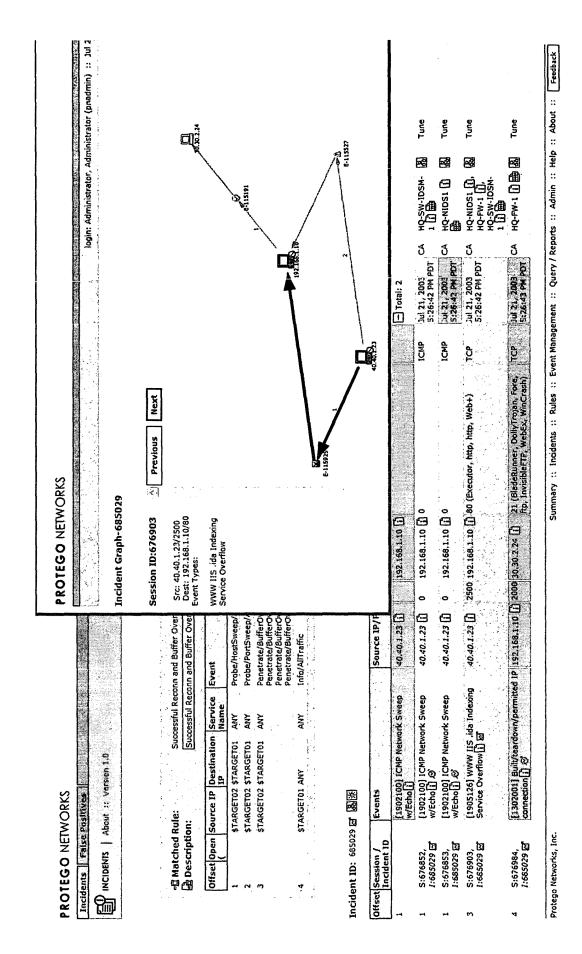


Fig. 13(C)

PROTEGO NETWORKS	TWORKS	3 Raw Events - Microsoft Internet Explorer	N HELP ABOUT
Incidents False Positives	e Positives		
SINCIDENIS	P INCIDENTS About 1: Version 1.0	PROTEGO NETWORKS	OT :: Activate
		login: Administrator, Administrator (priedmin) :: Jul 21, 2003 S:58 <u>136 FN</u> how:	10w Session ID
all Matched Bule.	Bulo Survestill Recons and Buffer	Raw Events	
Description:	j		
Offset Open	Offset Open Source IP Destination Service Event	Event / Reporting Time Raw Message Session / Device Incident ID	Time-range
ल त्य (ANY	E:676984, HQ-FW-1 Jul 21, 2003 10.33.10.2 < 142 > %PIX-6-302013: Built outbound TCP connection 2061 S:676984, 5:26:43 PM for dmz.192.168.1.10/2000 (100.1.4.12/2000) to outside:30.30.2.24/21 (30.30.2.24/21)	
"	STAKGETUZ ŞTAKGETUL ANY PENEGRAZIPUL Penetrate/Bur Penetrate/Bur Penetrate/Bur	HQ-FW-1 Jul 21, 2003 5:26:43 PM	· · .
4	\$TARGETO1 ANY ANY Info/AllTraffic	HQ-FW-1 Jul 21, 2003 10.33.10.2 <141-%PIX-6-303002: 192.168.1.10 Retrieved 5:26:43 PM 30.30.2.24:/ufl	Ohh:5mm:0ss
Incident ID: 635029 匠 뢻胀	29 匠 優麗	Protego Networks, Inc.	Escalate
Offset Session / Incident ID	Events	P/Port Destination IP/Port Graph False Protocol Time Zone Reporting Graph False Positive	re Mitigation Itive
H	[1902100] ICNP Network Sweep 46.40.1.23 [] w/Echo[]]	1 📗 1392.166.1.10 🗓	
1 5:676852,	(1902100) ICMP Network Sweep 40,40,1.23 w/Echo[j] &	3 ① 0 192.168.1.10 ① 0 10-5W-1DSM- 園 Tune 5:26:42 PM PDT 1 ① 画	:
1 S:676853,	[1902100] ICMP Network Sweep 40.40.1.2. w/Echo[] &	3 [] 0 192,168,1,10 [] 0 100 100 100 100 100 100 100 100 100	
3 S:676903, I:665029 百	(1905)26) WWW IIS .ida.Indexing 40.40.1.2 Service Overflow[]] 図	3	
4 S:676984, 1:685029 🗃	[1302001] BuilVeardown/permitted 1P 192,168.]	1.0 [] 2000 30.30.2.24 [] 21 (BladeRumer, DollyTrojan, Fore, TCP Jul 21, 2003 CA HQ-FW-1 [] 圖 過 Tune () 2004 30.30.2.24 [] 和 ftp, InvisibleFFP, WebEx, WinCrash)	
Protego Networks, Inc.)C.	Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About ::	out :: Feedback

Fig. 14(A)

Fig. 14(B)

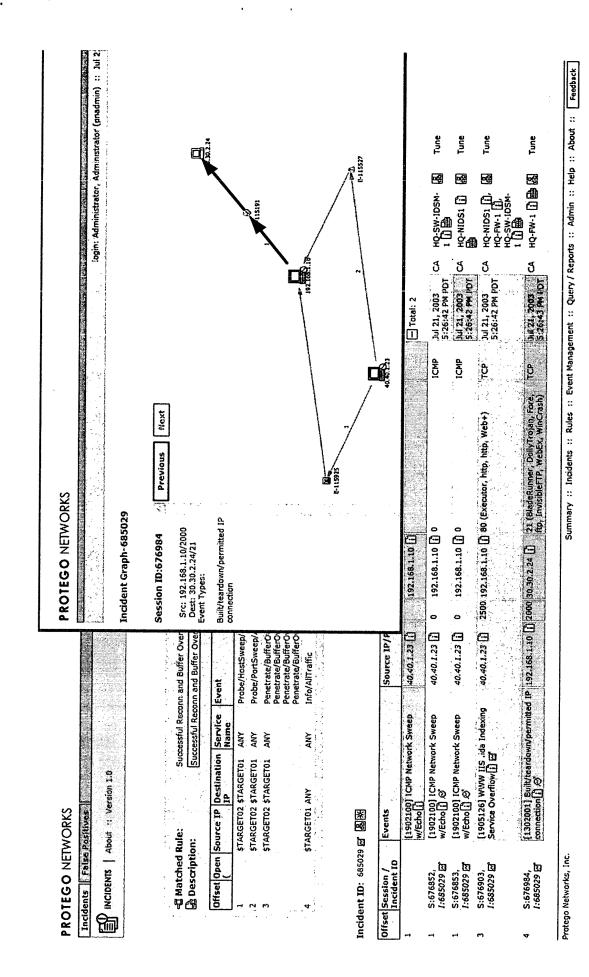


Fig 14(C)

PROTEGO NETWORKS	결 False Positive Confirm Page - Microsoft Internet Explorer	X
Incidents False Positives [PROTEGO NETWORKS	.1
-日 Matched Rule: Nimda Rule Bale Bale Bale Bale Offset Open (Source IP Destination 1 ANY ANY ANY ANY	False Positive Confirm Page Attack Type 'IIS Dot Dot Crash Attack' is valid for: Operating Systems: Windows NT 4.0 Applications: Internet Information Server (IIS) 2.0 Protocol: TCP	
Incident ID: 665008 缸 關胀	The record in the system detected that destination host Corp-web1 is running:	***********
Offset Session / Events Incident 10 Incide	Operating System: Windows 2000 Server ANY Service: Port: 80 (IP) Microsoft IIS 5.0 Host Info	
1:002000 因 Audack [] 2; (1903zila) WWW 11S Unicode (1903zila) WWW 11S Unicode (1905zila) WWW 11S Unicode (1905zila) WWW 11S Unicode (1905zila) WWW 11S Unicode (1905zila) WWW 11S Unicode (1) 位	As such, these events are determined to be False Positive. Is this determination correct? Yes C No C	
[1905124] IIS CGI Double Decode[]] [] 公 [1903215] IIS DOT DOT EXE Attack [],	Cancel	
[1903216] IIS Dot Dot Crast Attack[]], [1905081] WWW WinNT cmo Access[]], [1905114] WWW IIS Unicod Attack[], [1905124] IIS CGI Double Decode []	Protego Networks, Inc.	
Protego Networks, Inc.		۶٠.
3) <u>000 e</u>		

Fig. 15(A)

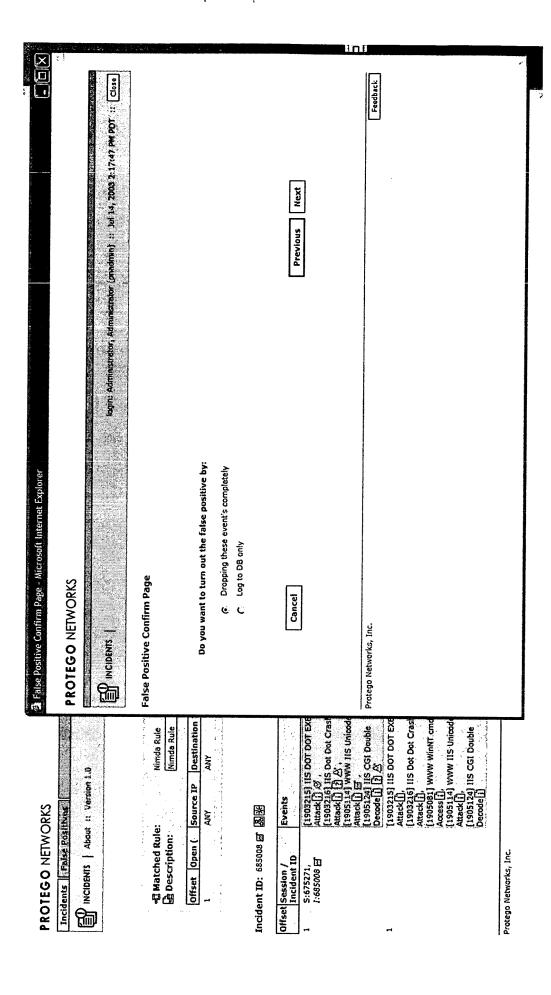


Fig. 15(B)

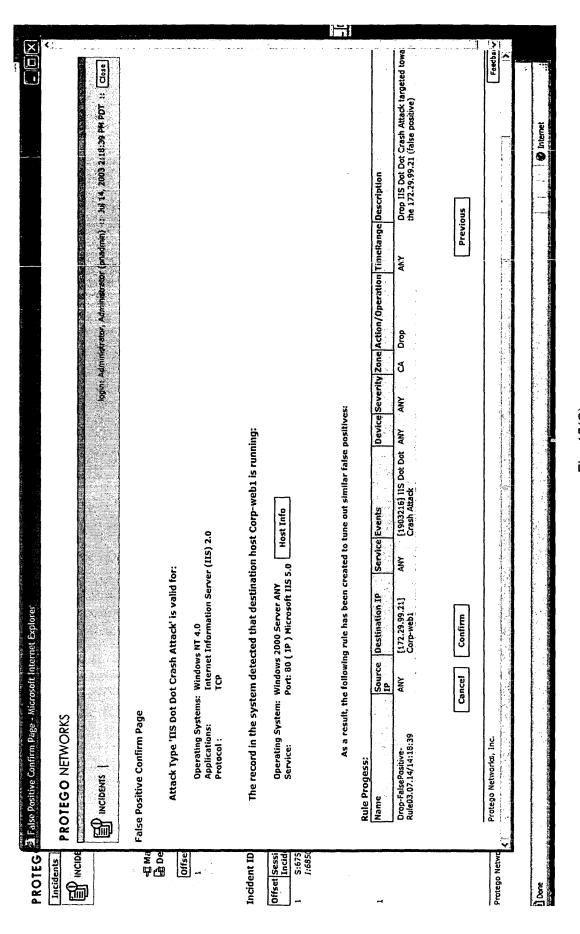


Fig. 15(C)

Incidents False Positives	titives	At the same	一种工作工作。						NE CHENNEL PROPERTY.	3000		40 C. Sel
MICTORNIS About :: Version 1.0	ugesen Tiesen				login: Admenstrator, Administrator (madmin) ::	or, Administra	tor (produm) ::	Treiger Legiont	11 304 14 2002 2 1945 PM PUT ::	2:19:45	# . .	Activate
					585008		Show Incident ID				Show Session ID	Sion ID
न्द्र Matched Rule: ङ्रि Description:	äi	Nimda Rule Nimda Rule		Herrical States of the Control of th	Complete the second sec			* *,				
Offset Open (Source IP	Destination IP	Service Name	Event	Device Ser	Severity Counts	Zone)	Close	Action/Operation	Γ	Time-range	
13	AMA	ANY		Penetrate/Nimdaworm	ANY ANY	in .	N	m	-Dage	5	0hh: 10mm:0ss] ,
Incident IO: 685008 罶	*											Escalate
Offset Session / Incident ID	Events		Source IP/Port	Destination IP/Port		Protocol Time	ne Te	Zone R	Zone Reporting	Graph False	False	Mitigation
·	(1993215] III Attack[] & (1993216] III Attack[] & (1995114] M Attack[] & (1995113] III Decode[] [] (1993215] III Attack[], (1993215] III Attack[], (1995134] M Attack[], (1995134] M Attack[], (1995134] III Decode[]	(1993215] IIS DOT DOT EXECUTE Attack[] Ø', (1993216] IIS DOT DOT Crash Attack[] [] Ø', (1995124] IIS CSI Double Attack[] Ø', (1995124] IIS DOT DOT EXECUTE Attack[], (1993215] IIS DOT DOT CRACUTE ATTACK[], (1993216] IIS DOT DOT CRACUTE ATTACK[], (199518] WWW WINNT CMG-EXE ACCESS[], (1995124] IIS CSI Double Attack[], (1995124] IIS CSI Double Decode[]	20.20.1.15 <u>1] 256</u>	() 2509 172.29.59.21 () 80 (htto, Web-1.	D.	M PD 72003 2:00:57 CA	1	A SK	E	Tune	
Protego Networks, Inc.				Summary ::	Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About ::	: : Event Mar	agement :: Qu	ery / Repo	rts :: Admin ::	Help ::	About ::	Feedback

Fig. 15(D)

logini: Administrator, Administrator (pnadmin) :: Lugout :: Jul 14, 2003 2:20:50 PM PDT :: Activate		Duplicate Add	Event Device Severity Zone Action/Operation Time- Description	[1905081] WWW WinNT ANY ANY CA Drop Auy Drop Www WinNT cmd.exe Access targeted cmd.exe Access	[1903216] IIS Dot Dot ANY ANY CA Drop ANY Drop IIS Dot Dot Crash Attack targeted Crash Attack	Duplicate Add	Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback
			Source Destination IP Service Event	[172,29,99.21] ANY Corp-web1	[172.29.99.21] ANY Corp-web1		
ARULES About :: Version 1.0		Change Status		Prop-FalsePositive- Rule03.07.11/16:38:05	Drop-FalsePositive- Rule03.07.14/14:18:39	Change Status	Inc.
RULES	Drop Rules:	Edit Chang	Status Rule Name	☐ 1 Drop-I Rule03	T 1 Drop-F	Edit Chang	Protego Networks, Inc.

Inspection Rules Drap Rules

Fig. 16(A)

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Freedback logini: Actorinistrator, Administrator (pradimin) 🟗 Logort 💸 10/14/2 2003 2::12:02 PM PGT 😭 Activate S Zg გ 1 to 2 of 2 25 per page Protocol ဦ ņ 80 80 Destination IP/Port 172,29,99,21 172.29.99.21 [1905081] WWW WiNNT cmd.exe Access [] [] & [1903216] IIS Dot Dot Crash Attack[]] 图 8: Event Select False Positive: Confirmed False Positive Type 1:415004 园, 1:415008 园, 1:550001 园, 1:550008 园, 1:550012 园, 1:685004 园, 1:685008 园 1:415004 國, 1:415008 國, 1:550001 國, 1:550008 國, 1:550012 國 MCIDENTS | About 3: Version 1.8 Incidents Protego Networks, Inc. Change Status Count ر ا S L

Fig. 16(B)

45 Mat	न्य Matched Rule:	Nimda Rule										٠	
B Des	Description:	Nimda Rule					-						
-								•					
Offset	Offset Open (Source IP	Destination IP	Service Name	Event	Device	Device Severity	Counts 20	Zone) Close	Action/Operation	Γ	Time-range	Ĺ	
***	ANY	ANY	ANY	Penetrate/Nimdaworm	ANY	ANY	S		Epage		0hh:10mm:0ss	} ,	
	-	•	ه چين طو د دوره ار مغرواستم به ده ده	enders geringelsender i de de enderske gemen Ammer de	The second second	a folio communicació contributo del				* * * * * * * * * * * * * * * * * * *	•		
Incident ID:	Incident ID: 665008 區 圖悉											Escalate	
Offset Session / Incident ID	n / Events nt IO		Source IP/Port	t Ocstination IP/Port		Protoco	Protocol Time	72	Zone Reporting Devices	Graph	Graph False Positive	Mitigation	
1 S:675271, 1:685005 図		[1903215] IIS DOT DOT EXECUTE Attack [] 197, [1903216] IIS Dot Dot Crash	8	24.16 [] 2509 172.29.99.21 [] 80 (Executor, http. http://ebs.f.)	vecutor, http Meb+)	<u>გ</u>	20114, 200 PM POT	Jul 14, 2003 2.00:S7 CA PN PDF	HQ-NIDS-2 D,	65 연 _수 :	Tune		
	🗿 Query - Microsoft Internet Explorer	ternet Explorer								the state of the s	the state of the s		X.0.
	File Edit View Favorites Tools Help	tes Tools Help							ŀ				20
***	Bed	S C C C C C C C C C C C C C C C C C C C	carch Stravailles	3 mas 3 3 3 3 3 3 3 3 3 3		•	The second secon	at the same of the same of			·		
	Address (2) http://10.1.1.129:8080/gui/Query/Index.jsp	29:8080/gui/Query/Index	Q	designament end parafestaren undersambateran den medisumen den austresam	and the second s		-		The second secon	***************************************	-		3
	FDA al Free Downloads 图 Downloads - 研Options	B Downloads - 研化	Childrens	odel @ Blood	■ Top Downloads •	Manusatods - @Heb	ods · ③Heb	Δ					
6 3	PROTEGO NETWORKS	WORKS				SUMMARY	INCIDENTS	RULES EVEN	EVENT MANAGEMENT	T QUERY & REPORTS	FROMS ADMIN	AIN HELP	ABOUT
	Query Report											100	and the
D. Explorer Sna	QUERY / REPORTS About :: Version 1.0	\$ About :: Vers	m 1.0		50	iogin: Administrator, Administrator (priadmin) :: Logout	sr, Administe	stor (pradmin	1: Logout	:: Jul 14, 200	11 Dul 14, 2003 2:32;06 PM PDT ::		Activate
[e		energia de la companya de la company	i de la companya de l	desir messi Vi desirandesiralenda dari karatar sami bari karatar karatar dari				Show Incident ID			ts	Show Session ID	91
first Sagi	Query Event Data Click the cells below to	Query Event Data Click the cells below to change query criteria:	riteria:										
2002 S00)	24		\$					· [Γ			:	·
3200. 3200. 320. 3200.	20.20.1.15	ANY ANY	ANY	EVENTS DEVICE SA	Severity	ANY Non	Vone	ANY ANY	<u> </u>	Time Range 1hh:0mm:0ss	Display Format Sessions	mat	
D.W.							Ц	Save As Report		Save As Rule	Gear	Submit	
ster With ochba	Protego Networks, Inc.	tworks, Inc.		Summ	ary :: Incid	ents :: Rules	:: Event M	anagement :	Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback	ts :: Admin	:: Help :: Ab	bout :: Fe	edback

Fig. 17(A)

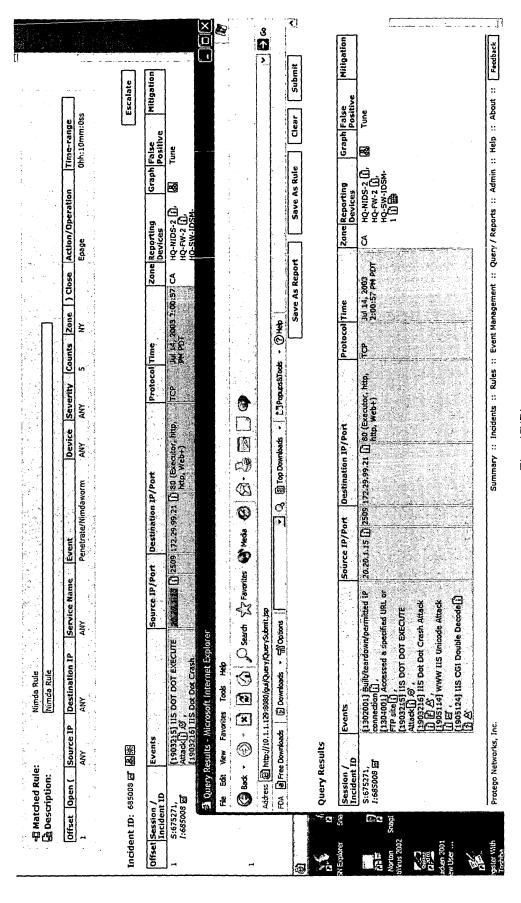


Fig. 17(B)

E nescubnou:	Nimda Rule	Raw Events - Microsoft Internet Explorer	rosoft Infernet	Explorer		
Offset Open (Source IP	e IP Destination IP Service Name ANY ANY				login: Administrator, Administrator	login: Administrator, Administrator (pnadmin) :: Jul 14, 2003 2:35:12 PM PDT :: Gose
	e indice and the results and a single management of admitting construction of the	Raw Events	American Ame			
Incident ID: 685008 日 國際						
Offset Session / Events	Source IP/Po	Event / Session / Incident ID	Reporting Device	Tìme	Raw Message	
2 6	S) IIS DOT DOT EXECUTE TOTAL	E:675271, S:675271, I:685008 EF	HQ-FW-2	Jul 14, 2003 2:00:57 PM PDT	172.29.100.4 <142> %PIX-6-302013 outside: 20.20.1.15/2509 (20.20.1.15	172.29.100.4 <142>%PIX-6-302013: Bullt inbound TCP connection 1978 for outside: 20.20.1.15/2509 (20.20.1.15/2509) to inside: 172.29.99.21/80 (100.1.64.21/80)
	1903216) IIS Dot Ook Chash	E:675278, S:675271, I:685008 🖼	HQ-FW-2	Jul 14, 2003 2:00:57 PM PDT	172.29.100.4 < 142.5 %PIX-6-302014: outside: 20.20.1.15/2509 to inside: 17	1/2,29,100.4 <142>%FIX-6-302014: Teardown TCP connection 1978 for outside: 20.20.1.15/2509 to inside: 172.29.99.21/80 duration 0:00:22 bytes 752 TCP Reset-O
Fire East Wave	Fire Edit Way Favorities Tooks Help Sect - (3) - (3) (3) (3) (3) Conductor	E:675272, S:675271, I:685008 🖼	HQ-FW-2	Jul 14, 2003 2:00:57 PM PDT	172.29.100.4 <141>%PIX-5-304301: 255c./%255c./%255c/%c1%1c. 1c./wint/system32/cmd.exe2/c+dir	172.29.100.4 <141>%PIX-5-304J01: 20.20.1.15 Accessed URL 100.1.54.21:/msadq/% 255c.,/%255c.,/%255c/%e1fsLc./%c1fsLc./%c1% 1c./winnt/system32/cmd.exe?/c+dir
Address (2) http://u	Address A http://10.1.1.1293050/gui/Query/QuerySubmit.jsp	E:675275, S:675271, I:685008 EF	HQ-NIDS-2	Jul 14, 2003 2:00:57 PM PDT	20.20.1.15/2509> 172.29.99.21/80	20.20.1.15/2509> 172.29.99.21/80 TCP IIS DOT DOT EXECUTE Attack
FDA S Free Downloads	bads (E) Downloads · Till Options	E:675268, S:675271, I:685008	HQ-SW- IDSM-1	Jul 14, 2003 2:00:57 PM PDT	20,20.1.15/2509> 100.1.64.21/80 TCP IIS DOT DOT EXECUTE Attack	I TCP IIS DOT DOT EXECUTE Attack
(Query Results		E:675276, S:675271,	HQ-NIDS-2	Jul 14, 2003 2:00:57 PM	20.20.1.15/2809> 172.29.99.21/80 TCP IIS Dat Dat Crash Attack	10 TCP IIS Dot Oot Crash Attack
Sna Session / Incident ID	Events	Source IP/Port Des	Destination IP/Port		Protocol Time Zon	Zone Reporting Graph False Mitigation Devices
Sie75271, Sie752	(1302001) Built/teardown/permitted IP 300 connection[], (1304001) Accessed a specified URL or FTP site[]. (130512) IIS DOT DOT EXECUTE (1305215) IIS DOT DOT EXECUTE (1305216) IIS DOT DOT Cresh Attack [] $\mathbb{D}[E]$ (1305216) IIS DOT DOT Cresh Attack [] $\mathbb{D}[E]$ (1305216) IIS DOT DOT Cresh Attack [] $\mathbb{D}[E]$ (1305214) WWW IIS Unicode Attack [] $\mathbb{D}[E]$ (1305214) IIS CGI Double Decode[]]	20.20.1.15 [] 2309 172.20.99.21 [] 80 (Executor, Mttp.)	26.99,21 <u>0</u>	80 (Executor, http., http., Web+)	TCP 14, 2003 2200,57 PN POT	HQ-NIDS-2 ①, 圆 HQ-NV-2 ①, HQ-SW-IDSH- 1 ① 圖

Fig. 17(C)